

<http://www.acrofan.com/ko-kr/consumer/content/?mode=view&cate=0303&wd=20111117&ucode=0003030201>



SEARCH

SEARCH

Home > Live > Report

## [취재] 2011 하반기 넷이벤츠 인터뷰 I : 소스파이어

[종목] 컴퓨터 [분야] IT일반 [작성자] 류재용 [작성일] 2011.11.17. 00:34

2011년 11월 16일과 17일 양일 간의 일정으로, 태국 푸켓 소재 인디고 펄 리조트(Indigo Pearl Resort, Phuket, Thailand)에서 '2011 넷이벤츠 아시아 태평양 기자간담회(2011 NetEvents APAC Press Summit, 이하 넷이벤츠)'가 개최되었다. 지난 4월에 열린 상반기 행사에 이어 열린, 11월 정례 하반기 행사다.

넷이벤츠는 통신 및 네트워크, 보안 기업의 C 레벨 임원들과 관련 시장조사기관이 한 자리에 모여 업계 동향 및 각 기업의 전략 등을 소개하는 정기행사다. 이번 행사에서는 엔터프라이즈 네트워킹, IT 보안, 무선 기술, 영상 회의, 클라우드 컴퓨팅, 차세대 통신망, 통신 인프라 등 업계 이슈에 관한 기업 및 시장 조사기관의 발표와 패널토론 등이 진행되었다.

16일 넷이벤츠의 오후일정은 업계 주요 인사들과의 인터뷰 시간으로 할애되었다. 아크로팬은 MEF 난 천 회장에 이어, 소스파이어 임직원들을 만날 수 있었다. 답변에는 레온 워드(Leon Ward) 필드 프로젝트 매니저, 스키야토 코(Sugiarto Koh) ASEAN 및 북아시아 지역 세일즈 디렉터, 가레스 마셜(Gareth Marshall) PR 담당자 등이 나섰다.



## 취재] 2011 하반기 넷이벤츠 인터뷰 II : 소스파이어

[종목] 컴퓨터 [분야] IT일반 [작성자] 류재용 [작성일] 2011.11.17. 00:34

2011년 11월 16일과 17일 양일 간의 일정으로, 태국 푸켓 소재 인디고 펄 리조트(Indigo Pearl Resort, Phuket, Thailand)에서 '2011 넷이벤츠 아시아태평양 기자간담회(2011 NetEvents APAC Press Summit, 이하 넷이벤츠)'가 개최되었다. 지난 4월에 열린 상반기 행사에 이어 열린, 11월 정례 하반기 행사다.

넷이벤츠는 통신 및 네트워크, 보안 기업의 C 레벨 임원들과 관련 시장조사기관이 한 자리에 모여 업계 동향 및 각 기업의 전략 등을 소개하는 정기행사다. 이번 행사에서는 엔터프라이즈 네트워킹, IT 보안, 무선 기술, 영상 회의, 클라우드 컴퓨팅, 차세대 통신망, 통신 인프라 등 업계 이슈에 관한 기업 및 시장 조사기관의 발표와 패널토론 등이 진행되었다.

16일 넷이벤츠의 오후일정은 업계 주요 인사들과의 인터뷰 시간으로 할애되었다. 아크로팬은 MEF 난 첸 회장에 이어, 소스파이어 임직원들을 만날 수 있었다. 답변에는 레온 와드(Leon Ward) 필드 프로젝트 매니저, 스키아토 코(Sugiarto Koh) ASEAN 및 북아시아 지역 세일즈 디렉터, 가레스 마샬(Gareth Marshall) PR 담당자 등이 나섰다.



▲ 가레스 마샬(왼쪽), 레온 와드(중앙), 스키아토 코(오른쪽)

Q1. (아크로팬) 한국은 중국발 해킹 피해가 크다. 그러면서 중국에서 들어오는 솔루션, 시그니처들도 날로 늘어나는 추세다. 문제는 중국에서 나오는 시그니처 패키지가 천 단위가 넘어 이를 튜닝하는 것을 일선 보안업체에서 어려워 하는 실정이다. 소스파이어는 날로 폭증하는 이러한 시그니처 관리와 튜닝 부분에서 어떻게 효율성을 높이는가?

소스파이어가 다른회사가 달리 하는 것이 있다. 고객 네트워크 환경에 대해서 가시성과 지식을 확보하는데 포커스를 두고 있다. 기술 중에서, 네트워크에 연결된 디바이스가 어떤 것이고, 돌아가는 운영체제 및 애플리케이션 등을 보고, 어떤 유저가 쓰고, 어떤 서비스가 제공되고 그러는지, 이런 부분들을 모두 자동으로 파악하는 기술이 있다. 이 기술을 사용해서 정보를 파악하고, 또 바탕으로 삼아서 어떤 시그니처를 쓸지 자동으로 연산, 계산해서 알 수 있게 해준다.

쓰고 있는 애플 노트북과 인텔 노트북이 취약점이 다르다. 네트워크 상에서 머신들이 어떤 커뮤니케이션을 하는지 잘 포착하고, 어택이 들어오면 디바이스가 어떻게 작동하고 운용되는지 수동적으로 파악하게 해준다. 수동적인 운영체제, 유저, 애플리케이션에 대한 디스커버리로 가시성을 확보한다.

일단, 어떠한 방식으로 환경을 보호하던간에 첫 단계는 현상파악이 된다. 보지를 못하면 보호도 못한다. 소스파이어 기술은 어떤 자산들이 보호대상인지 파악부터 한다. 그러한 가시성 확보를 바탕으로 여러 가지를 한다. 이 중에서 네트워크 보호를 위해 어떤 시그니처 이네이블을 선택하는 게 하나 있다. 또 얼럿을 해당 기업에 의미있는 방식으로 표시한다. 윈도우 취약점 어택이 들어오면 윈도우로 들어올 때하고 아이패드로 들어오는 건 의미가 다르다. 윈도우로 어택이 들어오면 윈도우 쓰는 회사에 경고를 알린다.

Q2. (아크로팬) 산업 측면에서 보면, 대기업이 채택한 보안정책, 솔루션이 기준이 되면서 하부 조직이나 기업까지 보안이 평준화되는 경향이 있다. 기업들은 비즈니스 관계를 감안해 기존 인트라넷 강화나 프라이빗 클라우드 이전을 고민하기도 한다. 이러한 여건 속에서, 소스파이어가 어떠한 사업기회를 포착할 수 있다고 보는가?

소스파이어에게 좋은 기회가 된다고 본다. 소스파이어는 네트워크에서 돌아가는 것은 모두 다 가시성 확보가 가능하다. 이런 기술을 통해, 본사 차원에서 규정 준수를 강행 준수로 요구할 수 있다. 일례로 파트너에서 sFTP를 쓰고자 한다면 이걸로 통일이 가능하다.

많은 대기업들이 소스파이어 기술을 써서 파트너, 지점, 지사들이 똑같은 수준의 보안수준을 강구하도록 해 나아가고 있다. 지사든 지역본부든 본사 보안수준이 지켜지도록 한다. 프로젝트는 소/중/대 박스가 있어서, 해당 환경에 맞춰 해당 소스를 쓸

수 있다. 본사나 지사나 동일 수준의 보안이 확보되도록 할 수 있다. 앞서 '박스'라고 표현했는데, 이는 센서다. 대기업에서는 전세계적으로 센서를 디플로이하고 디바이스 디플로이를 하게 된다. 전세계적으로 지사를 두고 있다면 이를 다 관리하는 게 이슈가 될텐데, 이를 다 확장가능성이 있게끔 해준다.